applications include an APACHE(TM) web server, SQL(TM)-based database management, various drivers and interface for the ports and other hardware, DHCP, IPB4 router, network access translation (NAT), a restrictive flow packet shaper, SNMP, point to point protocol (PPP), a virtual private network (VPN), a virtual LAN (VLAN), SSH tunneling. Some Open IP Services Platforms can also include a SAMBA server, DNS, a POP mail server, and full software or hardware RAID functionality.

**[0086]** The present invention also provides a standardized interface to all of the network cards that can be loaded. This interface is SQL-based to enable full control over access to the network functions. It is also a function of the invention to provide ActiveX modules for each network function that is being added. The power of this feature is that, for example, the ActiveX module can be input to a spreadsheet. As the network is operating, the spreadsheet is displaying all of the statistics of that network function in realtime.

**[0087]** One of the advantages of the present invention that may not yet be apparent is that it includes a central point of configuration control. Each network card has an

associated database and ActiveX component. Thus, two firewalls can be configured in exactly the same way. Obviously, each firewall card requires its own unique driver and instruction set because they are probably proprietary systems. Surprisingly, both of the firewall cards can be controlled using the identical ActiveX component and the same database. The present invention is able to provide a centralized, standard interface program that performs the translation between the database and the firewall cards themselves.

**[0088]** It was stated previously that the present invention provides allocation of network resources at the port, protocol, and IP address level. In other words, it is possible to control and thus sell IP services on a port-by-port basis. It is useful to examine several examples of how this works.

**[0089]** Consider an office building with four tenants, A, B, C and D. In a packet shaper that comes with the REACTOR(TM), each of the tenants can be allocated Internet access by a rule set, trigger point, or manually. Rule sets are used to allocate resources. For example, the tenants can share a T1 line equally, where each tenant is

restricted to 300 kb of bandwidth. A trigger point is used to activate particular rule sets, depending upon the conditions. Finally, it is possible to manually override the rule sets and trigger points.

**[0090]** A first example is when none of the tenants are restricted to the amount of bandwidth that they can use. Therefore, tenant A may use 800 kb of bandwidth without interfering with the other tenants. Then, tenants B, C, and D all need 200 kb of bandwidth. At this point, the bandwidth of the T1 is exceeded. A trigger point can be set so that when bandwidth demand exceeds the maximum available bandwidth, the tenants are restricted. The rule set that is activated can divide all the bandwidth equally, or still favor the heaviest bandwidth user while reducing the bandwidth to that user.

**[0091]** Bandwidth can also be allocated according to the type of activity that is being performed. Thus, activity can be restricted based on protocol, or the type of activity that is occurring. Thus, all tenants can be given unrestricted flow control on e-mail, but restricted flow on web browsing or FTP.

**[0092]** It was mentioned that flow control can be